

**UNITED STATES DISTRICT COURT  
DISTRICT OF NORTH DAKOTA**

**STEVEN ROBERTSON**, individually,  
and on behalf of all others similarly  
situated,

Plaintiff,

vs.

**FORUM COMMUNICATIONS  
COMPANY.,**

Defendant.

Case No.

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiff alleges as follows:

**INTRODUCTION**

1. Plaintiff Steven Robertson brings this Class Action Complaint against Defendant Forum Communications Company (“Defendant”) for its failure to properly secure and safeguard Plaintiff and Class Members’ protected personally identifiable information stored within Defendant’s information network, including, without limitation, names, Social Security numbers (“SSN”) and date of birth (these types of information, *inter alia*, being thereafter referred to, collectively, as “personally identifiable information” or “PII”).<sup>1</sup>

2. With this action, Plaintiff seeks to hold Defendant responsible for the harms it caused and will continue to cause Plaintiff and, at least, 28,830<sup>2</sup> other similarly situated persons

---

<sup>1</sup> Personally identifiable information (“PII”) generally incorporates information that can be used to distinguish or trace an individual’s identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual. PII also is generally defined to include certain identifiers that do not on its face name an individual, but that are considered to be particularly sensitive and/or valuable if in the wrong hands (for example, Social Security numbers, passport numbers, driver’s license numbers, financial account numbers, etc.).

<sup>2</sup> *Breach Portal*, <https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/788894ad-80a6-44b4-921c-16806027c921.html> (last accessed March 28, 2025).

in the massive and preventable cyberattack purportedly discovered by Defendant on February 21, 2025, in which cybercriminals infiltrated Defendant's inadequately protected network servers and accessed highly sensitive PII that was being kept unprotected ("Data Breach").

3. Plaintiff further seeks to hold Defendant responsible for not ensuring that PII was maintained in a manner consistent with industry standards.

4. While Defendant claims to have discovered the breach on or around February 21, 2025, Defendant did not inform victims of the Data Breach until March 19, 2025. Plaintiff and Class Members were wholly unaware of the Data Breach until they received letters from Defendant informing them of it.

5. Defendant acquired, collected, and stored Plaintiff and Class Members' PII. Therefore, at all relevant times, Defendant knew or should have known that Plaintiff and Class Members would use Defendant's services to store and/or share sensitive data, including highly confidential PII.

6. By obtaining, collecting, using, and deriving a benefit from Plaintiff and Class Members' PII, Defendant assumed legal and equitable duties to those individuals. These duties arise from state and federal statutes and regulations, and common law principles.

7. Defendant disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, and/or negligently failing to take and implement adequate and reasonable measures to ensure that Plaintiff and Class Members' PII was safeguarded, failing to take available steps to prevent unauthorized disclosure of data and failing to follow applicable, required and appropriate protocols, policies, and procedures regarding the encryption of data, even for internal use. As a result, Plaintiff and Class Members' PII was compromised through disclosure to an unknown and unauthorized third party—an undoubtedly nefarious third party seeking to profit off

this disclosure by defrauding Plaintiff and Class Members in the future. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe and are entitled to injunctive and other equitable relief.

### **JURISDICTION AND VENUE**

8. Jurisdiction is proper in this Court under 28 U.S.C. § 1332 (diversity jurisdiction). Specifically, this Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action where the amount in controversy exceeds the sum or value of \$5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one Class Member is a citizen of a state different from Defendant.

9. Defendant is headquartered and/or routinely conducts business in the State where this District is located, has sufficient minimum contacts in this State, has intentionally availed itself of this jurisdiction by marketing and/or selling products and/or services and/or by accepting and processing payments for those products and/or services within this State.

10. Venue is proper in this Court under 28 U.S.C. § 1391 because a substantial part of the events that gave rise to Plaintiff's claims took place within this District and Defendant is headquartered and/or does business in this Judicial District.

### **PLAINTIFF'S EXPERIENCES**

#### ***Plaintiff Steven Robertson's Experiences***

11. Plaintiff Steven Robertson is a former employee of the Defendant and is a citizen of Moorhead, Minnesota.

12. As a condition of his employment, Plaintiff Robertson was required to provide Defendant with his sensitive personal/private information, including, but not limited to, his name, Social Security number, and date of birth.

13. At the time of the Data Breach, Defendant retained Plaintiff's Private Information in its system.

14. Plaintiff Robertson is very careful about sharing his sensitive Private Information. Plaintiff stores any documents containing his Private Information in a safe and secure location. He has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff would not have entrusted his Private Information to Defendant had he known of Defendant's lax data security policies.

15. Plaintiff Robertson received the Notice Letter, by U.S. mail, directly from Defendant, dated March 19, 2025. According to the Notice Letter, Plaintiff's Private Information was improperly accessed and obtained by unauthorized third parties.

16. As a result of the Data Breach, and at the direction of Defendant's Notice Letter, Plaintiff has made reasonable efforts to mitigate the impact of the Data Breach, including researching and verifying the legitimacy of the Data Breach upon receiving the Notice Letter, changing passwords, and resecuring his own computer network, and contacting companies regarding suspicious activity on his accounts. Plaintiff Robertson has spent significant time dealing with the Data Breach—valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

17. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed him of key details about the Data Breach's occurrence.

18. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

19. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

20. Plaintiff Robertson has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

**DEFENDANT**

21. Defendant Forum Communications Company is a North Dakota corporation with its headquarters and principal place of business located at 101 5<sup>th</sup> Street N., Fargo, North Dakota 58102.

22. The true names and capacities of persons or entities, whether individual, corporate, associate or otherwise, who may be responsible for some of the claims alleged here are currently unknown to Plaintiff. Plaintiff will seek a leave of court to amend this Complaint to reflect the true names and capacities of such responsible parties when their identities become known.

**CLASS ACTION ALLEGATIONS**

23. Plaintiff brings this action pursuant to the provisions of Rules 23(a), (b)(2), and (b)(3) of the Federal Rules of Civil Procedure (“F.R.C.P.”) on behalf of Plaintiff and the following classe/subclass(es) (collectively, the “Class(es)”):

**Nationwide Class:**

“All individuals within the United States of America whose PII was exposed to unauthorized third parties as a result of the data breach discovered by Defendant on February 21, 2025.”

24. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant’s parents, subsidiaries, affiliates, officers, and directors and any entity in which Defendant has a controlling interest, all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out, any and all federal, state or local governments, including but not limited to its departments, agencies, divisions, bureaus, boards, sections, groups, counsel, and/or subdivisions, and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

25. In the alternative, Plaintiff requests additional subclasses as necessary based on the types of PII that were compromised.

26. Plaintiff reserves the right to amend the above Class definitions or to propose other subclasses in subsequent pleadings and motions for class certification.

27. This action has been brought and may properly be maintained as a class action under F.R.C.P. Rule 23 because there is a well-defined community of interest in the litigation and membership of the proposed Classe is readily ascertainable.

- a. Numerosity: A class action is the only available method for the fair and efficient adjudication of this controversy. The members of the Plaintiff Class are so numerous that joinder of all members is impractical, if not impossible. Plaintiff is informed and believes and, on that basis, alleges that the total number of Class Members is in the thousands of individuals. Membership in the Class will be determined by analysis of Defendant's records.
- b. Commonality: Plaintiff and the Class Members share a community of interest in that there are numerous common questions and issues of fact and law which predominate over any questions and issues solely affecting individual members, including, but not necessarily limited to:
  - 1) Whether Defendant had a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, using and/or safeguarding their PII;
  - 2) Whether Defendant knew or should have known of the susceptibility of its data security systems to a data breach;
  - 3) Whether Defendant's security procedures and practices to protect its systems were reasonable in light of the measures recommended by data security experts;
  - 4) Whether Defendant's failure to implement adequate data security measures allowed the Data Breach to occur;
  - 5) Whether Defendant failed to comply with its own policies and applicable laws, regulations and industry standards relating to data security;
  - 6) Whether Defendant adequately, promptly and accurately informed Plaintiff and Class Members that their PII had been compromised;
  - 7) How and when Defendant actually learned of the Data Breach;
  - 8) Whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the loss of the PII of Plaintiff and Class Members;

- 9) Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;
  - 10) Whether Defendant engaged in unfair, unlawful or deceptive practices by failing to safeguard Plaintiff and Class Members' PII;
  - 11) Whether Plaintiff and Class Members are entitled to actual and/or statutory damages and/or whether injunctive, corrective and/or declaratory relief and/or an accounting is/are appropriate as a result of Defendant's wrongful conduct;
  - 12) Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct.
- c. Typicality: Plaintiff's claims are typical of the claims of the Plaintiff Class. Plaintiff and all members of the Plaintiff Class sustained damages arising out of and caused by Defendant's common course of conduct in violation of law, as alleged herein.
  - d. Adequacy of Representation: Plaintiff in this class action is an adequate representative of each of the Plaintiff Class in that Plaintiff has the same interest in the litigation of this case as the Class Members, is committed to the vigorous prosecution of this case and has retained competent counsel who are experienced in conducting litigation of this nature. Plaintiff is not subject to any individual defenses unique from those conceivably applicable to other Class Members or the classes in their entirety. Plaintiff anticipates no management difficulties in this litigation.
  - e. Superiority of Class Action: The damages suffered by individual Class Members are significant but may be small relative to each member's enormous expense of individual litigation. This makes or may make it impractical for members of the Plaintiff Class to seek redress individually for the wrongful conduct alleged herein. Even if Class Members could afford such individual litigation, the court system could not. Should separate actions be brought or be required to be brought by each individual member of the Plaintiff Class, the resulting multiplicity of lawsuits would cause undue hardship and expense for the Court and the litigants. The prosecution of separate actions would also create a risk of inconsistent rulings which might be dispositive of the interests of other Class Members who are not parties to the adjudications and/or may substantially impede their ability to protect their interests adequately. Individualized litigation increases the delay and expense to all parties and to the court system, presented by the case's complex legal and factual issues. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale and comprehensive supervision by a single court.

28. Class certification is proper because the questions raised by this Complaint are of common or general interest affecting numerous persons, so it is impracticable to bring all Class Members before the Court.

29. This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to Class Members, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate concerning the Classes in their entirety. Defendant's policies and practices challenged herein apply to and affect Class Members uniformly. Plaintiff's challenge of these policies and procedures hinges on Defendant's conduct concerning the Classes in their entirety, not on facts or law applicable only to Plaintiff.

30. Unless a Class-wide injunction is issued, Defendant may continue failing to secure Class Members' PII properly, and Defendant may continue to act unlawfully, as set forth in this Complaint.

31. Further, Defendant has acted or refused to act on grounds generally applicable to the Classes and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under F.R.C.P. Rule 23(b)(2).

### **COMMON FACTUAL ALLEGATIONS**

#### **Defendant's Failed Response to the Data Breach**

32. Not until roughly four weeks after it claims to have discovered the Data Breach did Defendant begin sending the Notice to persons whose PII Defendant confirmed was potentially compromised because of the Data Breach. The Notice provided basic details of the Data Breach and Defendant's recommended next steps.

33. The Notice included, *inter alia*, the claims that Defendant had learned of the Data Breach on February 21, 2025, and had taken steps to respond. But the Notice lacked sufficient information on how the breach occurred, what safeguards have been taken since then to safeguard further attacks, and/or where the information hacked exists today.



34. Upon information and belief, the unauthorized third-party cybercriminals gained access to Plaintiff and Class Members' PII with the intent of misusing the PII, including marketing and selling Plaintiff and Class Members' PII.

35. Defendant had and continues to have obligations created applicable federal and state law as set forth herein, reasonable industry standards, common law, and its own assurances and representations to keep Plaintiff and Class Members' PII confidential and to protect such PII from unauthorized access.

36. Plaintiff and Class Members were required to provide their PII to Defendant to receive employment, and as part of providing employment Defendant created, collected, and stored Plaintiff and Class Members' PII with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

37. Despite this, even today, Plaintiff and Class Members remain in the dark regarding what data was stolen, the particular malware used, and what steps are being taken to secure their PII in the future. Thus, Plaintiff and Class Members are left to speculate as to where their PII ended up, who has used it, and for what potentially nefarious purposes. Indeed, they are left to further speculate as to the full impact of the Data Breach and how Defendant intends to enhance its information security systems and monitoring capabilities to prevent further breaches.

38. Plaintiff and Class Members' PII may end up for sale on the dark web or fall into the hands of companies that will use the detailed PII for targeted marketing without Plaintiff and/or Class Members' approval. Either way, unauthorized individuals can now easily access Plaintiff and Class Members' PII.

**Defendant Collected/Stored Plaintiff and Class Members' PII**

39. Defendant acquired, collected, stored, and assured reasonable security over Plaintiff and Class Members' PII.

40. As a condition of its relationships with Plaintiff and Class Members, Defendant required that Plaintiff and Class Members entrust Defendant with highly sensitive and confidential PII. Defendant, in turn, stored that information on Defendant's system that was ultimately affected by the Data Breach.

41. By obtaining, collecting, and storing Plaintiff and Class Members' PII, Defendant assumed legal and equitable duties over the PII and knew or should have known that it was thereafter responsible for protecting Plaintiff and Class Members' PII from unauthorized disclosure.

42. Plaintiff and Class Members have taken reasonable steps to maintain their PII's confidentiality. Plaintiff and Class Members relied on Defendant to keep their PII confidential and securely maintained, to use this information for business and employment purposes only, and to make only authorized disclosures of this information.

43. Defendant could have prevented the Data Breach, which began in early January 2025, by properly securing and encrypting and/or more securely encrypting its servers, generally, as well as Plaintiff and Class Members' PII.

44. Defendant's negligence in safeguarding Plaintiff and Class Members' PII is exacerbated by repeated warnings and alerts directed at protecting and securing sensitive data, as evidenced by the trending data breach attacks in recent years.

45. Data breaches such as the one experienced by Defendant have become so notorious that the Federal Bureau of Investigation (“FBI”) and the U.S. Secret Service have issued a warning to potential targets so they are aware of, can prepare for, and hopefully ward off a potential attack.

46. Due to the high-profile nature of these breaches and other breaches of its kind, Defendant was and/or certainly should have been on notice and aware of such attacks occurring in the healthcare industry and, therefore, should have assumed and adequately performed the duty of preparing for such an imminent attack.

47. And yet, despite the prevalence of public announcements of data breaches and data security compromises, Defendant failed to take appropriate steps to protect Plaintiff and Class Members’ PII from being compromised.

**Defendant Had a Duty to Protect the Stolen Information**

48. In failing to adequately secure Plaintiff and Class Members’ sensitive data, Defendant breached duties it owed Plaintiff and Class Members under statutory and common law. Moreover, Plaintiff and Class Members surrendered their highly sensitive personal data to Defendant under the implied condition that Defendant would keep it private and secure. Accordingly, Defendant also had an implied duty to safeguard their data, independent of any statute.

49. Defendant was also prohibited by the Federal Trade Commission Act (the “FTC Act”) (15 U.S.C. § 45) from engaging in “unfair or deceptive acts or practices in or affecting commerce.” The Federal Trade Commission (the “FTC”) has concluded that a company’s failure to maintain reasonable and appropriate data security for consumers’ sensitive personal information is an “unfair practice” in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

50. According to the FTC, the need for data security should be factored into all business decision-making. To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as Defendant, should employ to protect against the unlawful exposure of PII.

51. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business. The guidelines explain that companies should:

- a. protect the sensitive consumer information that they keep;
- b. properly dispose of PII that is no longer needed;
- c. encrypt information stored on computer networks;
- d. understand their network's vulnerabilities; and
- e. implement policies to correct security problems.

52. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

53. The FTC recommends that companies not maintain information longer than is necessary for authorization of a transaction, limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor for suspicious activity on the network and verify that third-party service providers have implemented reasonable security measures.

54. The FTC has brought enforcement actions against businesses for failing to protect consumer data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15

U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

55. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to consumers' PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

56. In addition to its obligations under federal and state laws, Defendant owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII in Defendant's possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendant owed a duty to Plaintiff and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected Plaintiff and Class Members' PII.

57. Defendant owed a duty to Plaintiff and Class Members to design, maintain, and test its computer systems, servers, and networks to ensure that all PII in its possession was adequately secured and protected.

58. Defendant owed a duty to Plaintiff and Class Members to create and implement reasonable data security practices and procedures to protect all PII in its possession, including not sharing information with other entities who maintain sub-standard data security systems.

59. Defendant owed a duty to Plaintiff and Class Members to implement processes that would immediately detect a breach of its data security systems in a timely manner.

60. Defendant owed a duty to Plaintiff and Class Members to act upon data security warnings and alerts in a timely fashion.

61. Defendant owed a duty to Plaintiff and Class Members to disclose if its computer systems and data security practices were inadequate to safeguard individuals' PII from theft, because such an inadequacy would be a material fact in the decision to entrust this PII to Defendant.

62. Defendant owed a duty of care to Plaintiff and Class Members because they were foreseeable and probable victims of any inadequate data security practices.

63. Defendant owed a duty to Plaintiff and Class Members to encrypt and/or more reliably encrypt Plaintiff and Class Members' PII and monitor user behavior and activity to identify possible threats.

**The Sensitive Information Stolen in the Data Breach is Highly Valuable**

64. It is well known that PII, including Social Security numbers particularly, is a valuable commodity and a frequent, intentional target of cybercriminals. Companies that collect such information, including Defendant, are well aware of the risk of being targeted by cybercriminals.

65. Individuals place a high value not only on their PII but also on the privacy of that data. Identity theft causes severe negative consequences to its victims, as well as severe distress and hours of lost time trying to fight the impact of identity theft.

66. While the greater efficiency of electronic records translates to cost savings for providers, it also comes with the risk of privacy breaches. These electronic health records contain a lot of sensitive information that is valuable to cybercriminals. One individual's complete record can be sold for hundreds of dollars on the dark web. As such, PII is a valuable commodity for which a "cyber black market" exists where criminals openly post stolen payment card numbers, Social Security numbers, and other personal information on several underground internet websites.

67. The high value of PII to criminals is evidenced by the prices they will pay for it through the dark web. For example, personal information can be sold at a price ranging from \$40 to \$200, and bank details have a price range of \$50 to \$200.<sup>3</sup> Experian reports that a stolen credit or debit card number can sell for \$5 to \$110 on the dark web.<sup>4</sup> Criminals can also purchase access to entire company data breaches from \$999 to \$4,995.<sup>5</sup>

68. These criminal activities have and will result in devastating financial and personal losses to Plaintiff and Class Members. For example, it is believed that certain PII compromised in the 2017 Experian data breach was being used three years later by identity thieves to apply for COVID-19-related benefits in Oklahoma. Such fraud will be an omnipresent threat for Plaintiff and Class Members for the rest of their lives. They will need to remain constantly vigilant.

69. The FTC defines identity theft as “a fraud committed or attempted using the identifying information of another person without authority.” The FTC describes “identifying information” as “any name or number that may be used, alone or in conjunction with any other information, to identify a specific person,” including, among other things, “[n]ame, Social Security number, date of birth, official State or government-issued driver’s license or identification number, alien registration number, government passport number, employer or taxpayer identification number.”

70. Identity thieves can use PII, such as that of Plaintiff and Class Members which Defendant failed to keep secure, to perpetrate various crimes that harm victims. For instance,

---

<sup>3</sup> *Your personal data is for sale on the dark web. Here’s how much it costs*, Digital Trends, Oct. 16, 2019, available at: <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/> (last accessed March 31, 2025).

<sup>4</sup> *Here’s How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, available at: <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/> (last accessed March 31, 2025).

<sup>5</sup> *In the Dark*, VPNOverview, 2019, available at: <https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/> (last accessed March 31, 2025).

identity thieves may commit various types of government fraud such as immigration fraud, obtaining a driver's license or identification card in the victim's name but with another's picture, using the victim's information to obtain government benefits, or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

71. The ramifications of Defendant's failure to secure Plaintiff and Class Members' PII are long-lasting and severe. Once PII is stolen, particularly identification numbers, fraudulent use of that information and damage to victims may continue for years. Indeed, the PII of Plaintiff and Class Members was taken by hackers to engage in identity theft or to sell it to other criminals who will purchase the PII for that purpose. The fraudulent activity resulting from the Data Breach may not come to light for years.

72. Individuals, like Plaintiff and Class Members, are particularly concerned with protecting the privacy of their Social Security numbers, which are the key to stealing any person's identity and are likened to accessing DNA for hacker's purposes.

73. Data breach victims suffer long-term consequences when their Social Security numbers are taken and used by hackers. Even if they know their Social Security numbers are being misused, Plaintiff and Class Members cannot obtain new numbers unless they become victims of Social Security misuse.

74. The Social Security Administration has warned that "a new number probably won't solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So, using a new number won't guarantee



you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.”<sup>6</sup>

75. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office (“GAO”), which conducted a study regarding data breaches:

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.<sup>7</sup>

76. When cybercriminals access financial information, health insurance information, and other personally sensitive data—as they did here—there is no limit to the amount of fraud to which Defendant may have exposed Plaintiff and Class Members.

77. Ultimately, data breaches are preventable.<sup>8</sup> As Lucy Thompson wrote in the DATA BREACH AND ENCRYPTION HANDBOOK, “[i]n almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions.”<sup>9</sup> She added that “[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised....”<sup>10</sup>

78. Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures. Appropriate information

---

<sup>6</sup> *Identity Theft and Your Social Security Number*, SSA, No. 05-10064 (July 2021), <https://www.ssa.gov/pubs/EN-05-10064.pdf> (last visited March 31, 2025).

<sup>7</sup> *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at*: <http://www.gao.gov/new.items/d07737.pdf> (last accessed March 31, 2025).

<sup>8</sup> Lucy L. Thompson, “Despite the Alarming Trends, Data Breaches Are Preventable,” *in* DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012)

<sup>9</sup> *Id.* at 17.

<sup>10</sup> *Id.* at 28.

security controls, including encryption, must be implemented, and enforced rigorously and disciplined so that a *data breach never occurs*.<sup>11</sup>

79. Here, Defendant knew of the importance of safeguarding PII and of the foreseeable consequences that would occur if Plaintiff and Class Members' PII was stolen, including the significant costs that would be placed on Plaintiff and Class Members because of a breach of this magnitude. As detailed above, Defendant knew or should have known that the development and use of such protocols was necessary to fulfill its statutory and common law duties to Plaintiff and Class Members. Therefore, its failure to do so is intentional, willful, reckless, and/or grossly negligent.

80. Furthermore, Defendant has offered only a limited one-year subscription for identity theft monitoring and identity theft protection through Experian. Its limitation is inadequate when the victims will likely face many years of identity theft.

81. Moreover, Defendant's credit monitoring offer and advice to Plaintiff and Class Members squarely place the burden on Plaintiff and Class Members, rather than on Defendant, to monitor and report suspicious activities to law enforcement. In other words, Defendant expects Plaintiff and Class Members to protect themselves from its tortious acts resulting from the Data Breach. Rather than automatically enrolling Plaintiff and Class Members in credit monitoring services upon discovery of the Data Breach, Defendant merely sent instructions to Plaintiff and Class Members about actions they could affirmatively take to protect themselves.

82. These services are wholly inadequate as they fail to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing

---

<sup>11</sup> *Id.*

identity theft and financial fraud, and they entirely fail to provide any compensation for the unauthorized release and disclosure of Plaintiff and Class Members' PII.

83. Defendant disregarded the rights of Plaintiff and Class Members by, *inter alia*: (i) intentionally, willfully, recklessly and/or negligently failing to take adequate and reasonable measures to ensure that its network servers were protected against unauthorized intrusions, (ii) failing to disclose that it did not have adequate security protocols and training practices in place to safeguard Plaintiff and Class Members' PII, (iii) failing to take standard and reasonably available steps to prevent the Data Breach, (iv) concealing the existence and extent of the Data Breach for an unreasonable duration of time, and (v) failing to provide Plaintiff and Class Members prompt and accurate notice of the Data Breach.

### **CAUSES OF ACTION**

#### **COUNT ONE**

##### **Negligence**

##### **(On behalf of the Nationwide Class)**

84. Each and every allegation of the foregoing paragraphs is incorporated in this Count with the same force and effect as though fully set forth herein.

85. At all times herein relevant, Defendant owed Plaintiff and Class Members a duty of care, *inter alia*, to act with reasonable care to secure and safeguard their PII and to use commercially reasonable methods to do so. Defendant took on this obligation upon accepting and storing Plaintiff and Class Members' PII on its computer systems and networks.

86. Among these duties, Defendant was expected:

- a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting the PII in its possession;
- b. to protect Plaintiff and Class Members' PII using reasonable and adequate security procedures and systems that were/are compliant with industry-standard practices;

- c. to implement processes to detect the Data Breach quickly and to act on warnings about data breaches timely; and
- d. to promptly notify Plaintiff and Class Members of any data breach, security incident or intrusion that affected or may have affected their PII.

87. Defendant knew or should have known that the PII was private and confidential and should be protected as private and confidential and, thus, Defendant owed a duty of care to not subject Plaintiff and Class Members to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

88. Defendant knew or should have known of the risks inherent in collecting and storing PII, the vulnerabilities of its data security systems and the importance of adequate security. Defendant knew or should have known about numerous well-publicized data breaches.

89. Defendant knew or should have known that its data systems and networks did not adequately safeguard Plaintiff and Class Members' PII.

90. Only Defendant was in the position to ensure that its systems and protocols were sufficient to protect the PII that Plaintiff and Class Members had entrusted to it.

91. Defendant breached its duties to Plaintiff and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard their PII.

92. Because Defendant knew that a breach of its systems could damage numerous individuals, including Plaintiff and Class Members, Defendant had a duty to adequately protect its data systems and the PII stored thereon.

93. Plaintiff and Class Members' willingness to entrust Defendant with their PII was predicated on the understanding that Defendant would take adequate security precautions. Moreover, only Defendant could protect its systems and the PII it stored on them from attack. Thus, Defendant had a special relationship with Plaintiff and Class Members.

94. Defendant also had independent duties under state and federal laws that required Defendant to reasonably safeguard Plaintiff and Class Members' PII and promptly notify them about the Data Breach. These "independent duties" are untethered to any contract between Defendant, Plaintiff, and/or the remaining Class Members.

95. Defendant breached its general duty of care to Plaintiff and Class Members in, but not necessarily limited to, the following ways:

- a. by failing to provide fair, reasonable and/or adequate computer systems and data security practices to safeguard Plaintiff and Class Members' PII;
- b. by failing to timely and accurately disclose that Plaintiff and Class Members' PII had been improperly acquired or accessed;
- c. by failing to adequately protect and safeguard PII by knowingly disregarding standard information security principles, despite obvious risks and by allowing unmonitored and unrestricted access to unsecured PII;
- d. by failing to provide adequate supervision and oversight of the PII with which it was and is entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted an unknown third party to gather Plaintiff and Class Members' PII, misuse the PII and intentionally disclose it to others without consent;
- e. by failing to adequately train its employees not to store PII longer than absolutely necessary;
- f. by failing to consistently enforce security policies aimed at protecting Plaintiff and Class Members' PII;
- g. by failing to implement processes to quickly detect data breaches, security incidents or intrusions; and
- h. by failing to encrypt Plaintiff and Class Members' PII and monitor user behavior and activity in order to identify possible threats.

96. Defendant's willful failure to abide by these duties was wrongful, reckless and/or grossly negligent in light of the foreseeable risks and known threats.

97. As a proximate and foreseeable result of Defendant's grossly negligent conduct, Plaintiff and Class Members have suffered damages and are at imminent risk of additional harm and damages (as alleged above).

98. The law further imposes an affirmative duty on Defendant to timely disclose the unauthorized access and theft of the PII to Plaintiff and Class Members so that they could and/or still can take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their PII.

99. Defendant breached its duty to notify Plaintiff and Class Members of the unauthorized access by waiting roughly three months after learning of the Data Breach to notify Plaintiff and Class Members and then by failing and continuing to fail to provide Plaintiff and Class Members sufficient information regarding the breach. To date, Defendant has not provided sufficient information to Plaintiff and Class Members regarding the extent of the unauthorized access and continues to breach its disclosure obligations to Plaintiff and Class Members.

100. Further, explicitly failing to provide timely and clear notification of the Data Breach to Plaintiff and Class Members, Defendant prevented Plaintiff and Class Members from taking meaningful, proactive steps to secure their PII and access their medical records and histories.

101. There is a close causal connection between Defendant's failure to implement security measures to protect Plaintiff and Class Members' PII and the harm (or risk of imminent harm suffered) by Plaintiff and Class Members. Plaintiff and Class Members' PII was accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII by adopting, implementing and maintaining appropriate security measures.

102. Defendant's wrongful actions, inactions, and omissions constituted (and continue to constitute) common law negligence.

103. The damages Plaintiff and Class Members have suffered (as alleged above) and will continue to suffer were and are the direct and proximate result of Defendant's grossly negligent conduct.

104. Additionally, 15 U.S.C. § 45 (FTC Act, Section 5) prohibits “unfair [...] practices in or affecting commerce,” including, as interpreted, and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendant’s duty in this regard.

105. Defendant violated 15 U.S.C. § 45 by failing to use reasonable measures to protect PII and by not complying with applicable industry standards, as described in detail herein. Defendant’s conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and Class Members.

106. Defendant’s violation of 15 U.S.C. § 45 constitutes negligence *per se*.

107. As a direct and proximate result of Defendant’s negligence and negligence *per se*, Plaintiff and Class Members have suffered and will continue to suffer injury, including but not limited to: (i) actual identity theft, (ii) the loss of the opportunity of how their PII is used, (iii) the compromise, publication, and/or theft of their PII, (iv) out-of-pocket expenses associated with the prevention, detection and recovery from identity theft, tax fraud, and/or unauthorized use of their PII, (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from embarrassment and identity theft, (vi) lost continuity in relation to their private information, (vii) the continued risk to their PII, which may remain in Defendant’s possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff and Class Members’ PII in its continued possession, and (viii) future

costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

108. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including but not limited to anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

109. Additionally, as a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and Class Members have suffered and will continue to suffer the continued risks of exposure of their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect PII in its continued possession.

**COUNT TWO**  
**Negligence *Per Se***  
**(On behalf of the Nationwide Class)**

110. Each and every allegation of the foregoing paragraphs is incorporated in this Count with the same force and effect as though fully set forth herein.

111. Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45 prohibits companies such as Defendant from "using any unfair method of competition or unfair or deceptive act or practice in or affecting commerce," including failing to use reasonable measures to protect PII. In addition to the FTC Act, the agency also enforces other federal laws relating to consumers' privacy and security. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.



112. In addition to the FTC rules and regulations and state law, other states, and jurisdictions where victims of the Data Breach are located require that Defendant protect PII from unauthorized access and disclosure and timely notify the victim of a data breach.

113. Defendant violated FTC rules and regulations obligating companies to use reasonable measures to protect PII by failing to comply with applicable industry standards and by unduly delaying reasonable notice of the actual breach. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of a Data Breach and the exposure of Plaintiff and Class members' highly sensitive PII.

114. Defendant's statutory violations of Section 5 of the FTC Act and other applicable statutes, rules and regulations, constitute negligence *per se*.

115. Plaintiff and Class Members are within the category of persons that the FTC Act were intended to protect.

116. The harm that occurred because of the Data Breach described herein is the type of harm that the FTC Act were intended to guard against.

117. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and Class Members have been damaged as described herein, continue to suffer injuries as detailed above, are subject to the continued risk of exposure of their PII in Defendant's possession and are entitled to damages in an amount to be proven at trial.

**COUNT THREE**  
**Breach of Confidence**  
**(On behalf of the Nationwide Class)**

118. Each and every allegation of the foregoing paragraphs is incorporated in this Count with the same force and effect as though fully set forth herein.

119. During Plaintiff and Class Members' interactions with Defendant, Defendant was fully aware of the confidential nature of the PII that Plaintiff and Class Members provided to it.

120. As alleged herein and above, Defendant's relationship with Plaintiff and Class Members was governed by promises and expectations that Plaintiff and Class Members' PII would be collected, stored, and protected in confidence, and would not be accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized third parties.

121. Plaintiff and Class Members provided their respective PII to Defendant with the explicit and implicit understandings that Defendant would protect and not permit the PII to be accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized third parties.

122. Plaintiff and Class Members also provided their PII to Defendant with the explicit and implicit understanding that Defendant would take precautions to protect their PII from unauthorized access, acquisition, appropriation, disclosure, encumbrance, exfiltration, release, theft, use, and/or viewing, such as following basic principles of protecting its networks and data systems.

123. Defendant voluntarily received, in confidence, Plaintiff and Class Members' PII with the understanding that the PII would not be accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by the public or any unauthorized third parties.

124. Due to Defendant's failure to prevent, detect and avoid the Data Breach from occurring by, *inter alia*, not following best information security practices to secure Plaintiff and Class Members' PII, Plaintiff and Class Members' PII was accessed by, acquired by, appropriated

by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized third parties beyond Plaintiff and Class Members' confidence and without their express permission.

125. As a direct and proximate cause of Defendant's actions and/or omissions, Plaintiff and Class Members have suffered damages, as alleged herein.

126. But for Defendant's failure to maintain and protect Plaintiff and Class Members' PII in violation of the parties' understanding of confidence, their PII would not have been accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized third parties. The Data Breach was the direct and legal cause of the misuse of Plaintiff and Class Members' PII and the resulting damages.

127. The injury and harm Plaintiff and Class Members suffered and will continue to suffer was the reasonably foreseeable result of Defendant's unauthorized misuse of Plaintiff and Class Members' PII. Defendant knew its data systems and protocols for accepting and securing Plaintiff and Class Members' PII had security and other vulnerabilities that placed Plaintiff and Class Members' PII in jeopardy.

128. As a direct and proximate result of Defendant's breaches of confidence, Plaintiff and Class Members have suffered and will continue to suffer injury, as alleged herein, including but not limited to: (i) actual identity theft, (ii) the compromise, publication, and/or theft of their PII, (iii) out-of-pocket expenses associated with the prevention, detection and recovery from identity theft and/or unauthorized use of their PII, (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft, (v) the continued risk to their PII, which

remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Class Members' PII in its continued possession, (vi) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiff and Class Members, (vii) the diminished value of Plaintiff and Class Members' PII, and (viii) the diminished value of Defendant's services for which Plaintiff and Class Members paid and received.

**COUNT FOUR**  
**Breach of Implied Contract**  
**(On behalf of the Nationwide Class)**

129. Each and every allegation of the foregoing paragraphs is incorporated in this Count with the same force and effect as though fully set forth herein.

130. Through their course of conduct, Defendant, Plaintiff and Class Members entered into implied contracts for Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiff and Class Members' PII.

131. Defendant required Plaintiff and Class Members to provide and entrust his PII as a condition of obtaining Defendant's employment services.

132. Defendant solicited and invited Plaintiff and Class Members to provide their PII as part of Defendant's regular business practices. Plaintiff and Class Members accepted Defendant's offers and provided their PII to Defendant.

133. As a condition of being Defendant's direct employees, Plaintiff and Class Members provided and entrusted their PII to Defendant. In so doing, Plaintiff and Class Members entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such non-public information, to keep such information secure and confidential and to timely and accurately notify Plaintiff and Class Members if their data had been breached and compromised or stolen.

134. A meeting of the minds occurred when Plaintiff and Class Members agreed to, and did, provide their PII to Defendant, in exchange for, amongst other things, the protection of their PII.

135. Plaintiff and Class Members fully performed their obligations under the implied contracts with Defendant.

136. Defendant breached the implied contracts it made with Plaintiff and Class Members by failing to safeguard and protect their PII and by failing to provide timely and accurate notice to them that their PII was compromised because of the Data Breach.

As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and Class Members have suffered and will continue to suffer: (i) ongoing, imminent and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm, (ii) actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm, (iii) loss of the confidentiality of the stolen confidential data, (iv) the illegal sale of the compromised data on the dark web, (v) lost work time, and (vi) other economic and non-economic harm.

**COUNT FIVE**  
**Breach of the Implied Covenant of Good Faith and Fair Dealing**  
**(On behalf of the Nationwide Class)**

137. Each and every allegation of the foregoing paragraphs is incorporated in this Count with the same force and effect as though fully set forth herein.

138. Every contract in this State has an implied covenant of good faith and fair dealing. This implied covenant is an independent duty and may be breached even when there is no breach of a contract's actual and/or express terms.

139. Plaintiff and Class Members have complied with and performed all conditions of their contracts with Defendant.

140. Defendant breached the implied covenant of good faith and fair dealing by failing to maintain adequate computer systems and data security practices to safeguard PII, failing to timely and accurately disclose the Data Breach to Plaintiff and Class Members, and continued acceptance of PII and storage of other personal information after Defendant knew or should have known of the security vulnerabilities of the systems that were exploited in the Data Breach.

141. Defendant acted in bad faith and/or with malicious motive in denying Plaintiff and Class Members the full benefit of their bargains as originally intended by the parties, thereby causing them injury in an amount to be determined at trial.

**COUNT SIX**  
**Breach of Fiduciary Duty**  
**(On behalf of the Nationwide Class)**

142. Each and every allegation of the foregoing paragraphs is incorporated in this Count with the same force and effect as though fully set forth herein.

143. In light of the special relationship between Defendant and Plaintiff and Class Members, whereby Defendant became the guardian of Plaintiff and Class Members' PII, Defendant became a fiduciary by its undertaking and guardianship of the PII to act primarily for Plaintiff and Class Members, (i) for the safeguarding of Plaintiff and Class Members' PII, (ii) to timely notify Plaintiff and Class Members of a data breach and disclosure, and (iii) to maintain complete and accurate records of what information (and where) Defendant did has and continues to store.

144. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of its relationship with its employees and former employees—in particular, to keep their PII secure.

145. Defendant breached its fiduciary duties to Plaintiff and Class Members by failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period of time.

146. Defendant breached its fiduciary duties to Plaintiff and Class Members by failing to encrypt and otherwise protect the integrity of the systems containing Plaintiff and Class Members' PII.

147. Defendant breached its fiduciary duties to Plaintiff and Class Members by failing to timely notify and/or warn Plaintiff and Class Members of the Data Breach.

148. Defendant breached its fiduciary duties to Plaintiff and Class Members by otherwise failing to safeguard Plaintiff and Class Members' PII.

149. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class Members have suffered and will continue to suffer injury, including but not limited to: (i) actual identity theft, (ii) the compromise, publication, and/or theft of their PII, (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PII, (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, contest, and recover from identity theft, (v) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession, (vi) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiff and Class Members, and (vii) the diminished value of Defendant's services they received.

150. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

**COUNT SEVEN**  
**Unjust Enrichment**  
**(On behalf of the Nationwide Class)**

151. Each and every allegation of the foregoing paragraphs is incorporated in this Count with the same force and effect as though fully set forth herein.

152. Upon information and belief, Defendant funds its data-security measures entirely from its general revenue.

153. Plaintiff and Class Members conferred a monetary benefit to Defendant. Specifically, they worked for the Defendant and/or its agents and provided Defendant with their PII. In exchange, Plaintiff and Class Members should have their PII protected with adequate data security.

154. Defendant knew that Plaintiff and Class Members conferred a benefit which Defendant accepted. Defendant profited from this employment relationship and used the PII of Plaintiff and Class Members for business purposes.

155. Defendant enriched itself by saving the costs it reasonably should have expended in data-security measures to secure Plaintiff and Class Members' PII. Instead of providing a reasonable level of security that would have prevented the hacking incident, Defendant instead calculated to increase its own profits at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. On the other hand, Plaintiff and Class Members suffered as a direct and proximate result of Defendant's decision to prioritize its profits over the requisite security.



156. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures mandated by industry standards.

157. Defendant failed to secure Plaintiff and Class Members' PII and, therefore, did not provide full compensation for the benefit of Plaintiff and Class Members.

158. Defendant acquired the PII through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

159. If Plaintiff and Class Members knew that Defendant had not reasonably secured their PII, they would not have agreed to provide their PII to Defendant.

160. Plaintiff and Class Members have no remedy at law.

161. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer injury, including but not limited to: (i) actual identity theft, (ii) the loss of opportunity to determine how their PII is used, (iii) the compromise, publication, and/or theft of their PII, (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII, (v) lost opportunity costs associated with efforts expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft, (vi) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect PII in its continued possession, and (vii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the impact of the PII

compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

162. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

163. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that it unjustly received from them.

### **RELIEF SOUGHT**

**WHEREFORE**, Plaintiff, on behalf of himself and each member of the proposed National Class respectfully request that the Court enter judgment in their favor and for the following specific relief against Defendant as follows:

1. That the Court declare, adjudge, and decree that this action is a proper class action and certify each of the proposed classes and/or any other appropriate subclasses under F.R.C.P. Rule 23 (b)(1), (b)(2), and/or (b)(3), including the appointment of Plaintiff's counsel as Class Counsel;

2. For an award of damages, including actual, nominal, and consequential damages, as allowed by law in an amount to be determined;

3. That the Court enjoin Defendant, ordering it to cease and desist from similar unlawful activities;

4. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff and Class Members' PII, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiff and Class Members;

5. For injunctive relief requested by Plaintiff, including but not limited to injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an Order:

- a. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;
- b. requiring Defendant to protect, including through encryption, all data collected through the course of business in accordance with all applicable regulations, industry standards and federal, state or local laws;
- c. requiring Defendant to delete and purge Plaintiff and Class Members' PII unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;
- d. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of Plaintiff and Class Members' PII;
- e. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring, simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis;
- f. prohibiting Defendant from maintaining Plaintiff and Class Members' PII on a cloud-based database;
- g. requiring Defendant to segment data by creating firewalls and access controls so that, if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;
- h. requiring Defendant to conduct regular database scanning and securing checks;
- i. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling PII, as well as protecting the PII of Plaintiff and Class Members;
- j. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs and systems for protecting personal identifying information;
- k. requiring Defendant to implement, maintain, review and revise as necessary a threat management program to monitor Defendant's networks for internal and external threats appropriately, and assess whether monitoring tools are properly configured, tested and updated;
- l. requiring Defendant to meaningfully educate all Class Members about the threats they face as a result of the loss of their confidential PII to third

parties, as well as the steps affected individuals must take to protect themselves.

6. For prejudgment interest on all amounts awarded, at the prevailing legal rate;
7. For an award of attorney's fees, costs, and litigation expenses, as allowed by law;
8. For all other Orders, findings and determinations identified and sought in this Complaint.

### **JURY DEMAND**

Plaintiff, individually and on behalf of the Plaintiff Class(es) and/or Subclass(es), hereby demand a trial by jury for all issues triable by jury.

Dated: April 2, 2025

By: /s/ Todd Miller

TODD MILLER (ND #06625)  
**SOLBERG STEWART MILLER**  
[tmiller@solberglaw.com](mailto:tmiller@solberglaw.com)  
1123 Fifth Avenue South  
P.O. Box 1897  
Fargo, ND 58107-1897  
Phone: (701) 237-3166  
Fax: (701) 237-4627

Philip J. Krzeski\**(pro hac vice admission forthcoming)*  
**CHESTNUT CAMBRONNE, P.A.**  
100 Washington Ave S., Unit 1700  
Minneapolis, Minnesota 55401  
Telephone: (612) 339-7300  
Email: [pkrzeski@chestnutcambronne.com](mailto:pkrzeski@chestnutcambronne.com)

*Counsel for Plaintiff and the Proposed Class(es)*